B

DRAFT EXECUTIVE ORDER TO GOVERN

ACCESS TO CLASSIFIED INFORMATION

2 February 1987

Declassified and Approved For Release 2012/11/28 : CIA-RDP89B01356R000100180005-5

Summary of Order

There are a number of personnel security and loyalty programs currently in existence. Except for the general requirement of section 4.1(a) of Executive Order 12356 that persons with access to classified information be determined trustworthy by agency heads or their designees and have an essential need for access, however, no single program governs the standards, procedures and authorities for such access. */ Thus, there is no coordinated government-wide policy concerning numbers of access approvals, investigative and adjudicative standards, or oversight responsibilities.

The new Order would create a government-wide policy and increase the protection afforded classified information in a number of ways. It separates determinations on access to classified information from suitability for federal employment. This will provide greater flexibility and discretion to the access program by insulating it from the procedural and substantive legal constraints that attach to adverse employment actions.

In addition, the Order will establish for the first time minimum investigative standards that all agencies must meet or exceed. The result will be more thorough background investigations in an area where many investigations, particularly for Secret level access, are currently woefully inadequate. More importantly, periodic reinvestigations would have the same priority as initial investigations, thus addressing the fact that most recent cases of espionage have been influenced by factors, such as financial instability, that develop after the initial investigation. At the present time, only a limited number of personnel are ever reinvestigated.

In a further effort to identify problems in advance, additional responsibilities will be placed on all persons, including supervisors, to report certain types of conduct and security violations. Finally, and most importantly, the Order creates a comprehensive oversight mechanism to promote uniform investigative and adjudicative criteria, provide training to investigators and adjudicators, and ensure adherence to the Order.

---

*/ Executive Order 10450, "Security Requirements for Government Employees," for example, established a federal employment security program under the broad oversight responsibility of OPM. That Order, however, addresses only employment and continued employment and not the more narrow and subtle questions of access - or denial of access - to classified information. Moreover, it is applicable only to government civilian employees as opposed to military or contractor personnel.

A detailed outline of the proposed Order follows.

* * * *

I. Access to Classified Information

A. Access determination

1. Separate from suitability or other security determinations

2. Kept to absolute minimum required

3. Granted only where necessary to perform official duties

a. Performance of this function by supervisors to be included in annual performance ratings

b. Not to be given solely to permit entry to controlled areas

c. Not to be requested based on a speculative need

B. Level of access approval

1. Granted at three levels = Top Secret, Secret and Confidential

2. Access to special access programs to be governed by agency heads who establish programs

C. Limited access to higher levels without further investigation

1. Where necessary to meet exigencies not of a recurring nature

2. Not to exceed 60 days

3. Limited to specific information

D. Observance of access determinations by other agencies

1. Determinations to be honored

2. Except where substantial derogatory information exists

E. Specific access requirement - "need to know" to be strictly enforced

II. Determination of Eligibility For Access

A. Based on completed background investigation

B. Personal and professional history affirmatively indicates enumerated, positive characteristics

C. Access by aliens

1. Limited access authorizations only

2. No greater level of access than can be given to country of origin

3. Prior ten years of life must be investigated

4. Exceptions by senior official only

III. Investigative Standards

A. Initial investigations

1. Secret and Confidential information

a. Review of U.S. Government records

b. Written inquiries of financial and credit sources and present and former employers

c. Check of state and local agencies

d. Degrees and diplomas confirmed

2. Top Secret information - expanded investigation

a. All of the above but with personal contacts

b. Personal interview of subject

c. Inquiries of other relevant sources of information (neighbors or coworkers)

3. Cover at least prior seven years

4. All questionable information to be fully pursued through any lawful investigative procedure

5. In emergencies, duties may be performed prior to completed background investigation

   a. Completely justified in writing

   b. Based on personal interview, review of FBI files, and contact with last employer

   c. For 120 days only - one 60 day-extension permitted

   d. Limited to particular, identified categories of information

6. Access at same level may be reapproved without investigation

   a. Deemed eligible for access within past five years

   b. Remained with same employer (or retired less than one year from Government

   c. Employer aware of no derogatory information

B. Reinvestigations

1. Requirements

   a. Same priority as initial investigations

   b. Frequency

      1) Anytime facts warrant

      2) Top Secret - every five years

      3) Secret and Confidential - at least every 10 years

   c. Updated personal history statements

      1) No less than every five years

      2) Whenever there is a significant change of circumstances

   d. Derogatory information to be sent to agency that granted access

2. Investigative techniques

a. Top Secret

1) Personal interview

2) Review of U.S. Government records

3) Local agency checks

4) Inquiries of financial and credit sources

5) Inquiries of persons familiar with subject

b. Secret and Confidential - as above except for personal interview

IV. Background Investigations for Foreign Governments

A. To facilitate background investigations in foreign countries on behalf of U.S.

B. Only with consent of the subject

V. Adjudication Criteria

A. General factors to be considered

1. Absence of exploitable vulnerabilities or conduct

2. Demonstrated trustworthiness, reliability and judgment

3. Criminal history

4. Alcohol or substance abuse

5. Financial and mental stability

6. Unquestioned loyalty

7. Susceptibility to influence, coercion or duress

B. Activities of other persons or groups also considered

1. Immediate family

2. Close ties of affection

3. Close and continuing contact

C. Access to be denied where reasonable doubt cannot be resolved by further investigation

D. Effect of adjudication - denial of access does not disqualify person for federal employment where access is not required

VI. Appeals

A. Need for access - within agency discretion and conclusive

B. Eligibility for access (denial or revocation)

1. General

a. Written explanation consistent with national security

b. Opportunity to reply in writing and request second review

c. Written notice of results of second review

d. Opportunity to appeal to higher authority (decision final)

2. Discretionary authority - agencies may provide additional proceedings

3. Exceptions

a. No appeal where senior official certifies an appeal would damage national security

b. No appeal at CIA and NSA where not in national interest

VII. Implementation And Review

A. Overall policy direction at NSC

B. Information Security Oversight Office (GSA)

1. Develop implementing directives, subject to NSC approval

2. Oversee agency actions to ensure compliance

3. Review agency implementing regulations for consistency with Order (decisions may be appealed to NSC)

4. Conduct on-site reviews of personnel security programs (access can be denied where there is an exceptional national security risk; ISOO can appeal to NSC)

5. Monitor adjudication policies and number of access approvals

6. Prescribe standard forms

7. Report annually to President

C. Agencies

1. Designate senior official to administer program

2. Promulgate implementing regulations

3. Any use of polygraph must

a. Limit dissemination of results

b. Ensure accurate results

c. Limit scope to counterintelligence questions

d. Inform subject of 5th Amendment rights

4. Establish training programs

5. Referral indications of espionage to FBI

D. Individuals with access

1. Report all contacts with persons who seek unauthorized access

2. Report all foreign travel

3. Report all violations of security regulations

4. Challenge questionable requests for access eligibility

E. Supervisors

1. Continually assess employees with access for conduct of concern

2. Report sudden affluence, unexplained foreign travel, excessive indebtedness, drug use, or excessive use of alcohol

VIII. General

A. Provisos

1. Any lawful investigative procedures may be utilized

2. CIA, NSA and FBI polygraph authorities unaffected

3. Atomic Energy Act to be adhered to

4. Temporary, limited access may be granted for specific intelligence or counterintelligence operations

5. Order does not apply to members of Congress or federal judges

B. Interpretation - by Attorney General

C. Revocation - Sections 2-9 of E.O. 10865, "Safeguarding Classified Information In Industry" (appeal process and rights)

Persons with access to national security information (also referred to as "classified information"), as defined in Executive Order 12356 of April 2, 1982 or its successors, are potential targets for foreign intelligence services that are engaged in sustained efforts to use human sources for access to such information. Even inadvertent disclosures of such information can reasonably be expected to cause damage to the national security. The decision to allow such access is, therefore, a wholly discretionary security determination that is independent of the personnel decision concerning whether a person is suitable for federal employment. This Order establishes a uniform federal personnel security program concerning those individuals who will be considered for access to national security information. Access to such information is not a right or entitlement, but is instead dependent upon established need for access and affirmative evidence of loyalty to the United States, strength of character, trustworthiness, reliability, discretion and sound judgment, as well as demonstrated freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use and handling of national security information. This Order is applicable to all United States Government employees, contractors, licensees, grantees, military personnel and other individuals (including applicants for Government positions) with an officially determined need for access.

By the authority vested in me as President by the Constitution and laws of the United States of America, and in order to enhance the national security of the United States by improving its personnel security policies, practices and programs, it is hereby ordered as follows:

Part 1

Access to National Security Information

Section 1.1 Access Determinations

(a) Determinations of eligibility for access to classified national security information shall be based on the criteria set forth in this Order and are totally separate from suitability or other security determinations with respect to the hiring or retention of persons for employment by the Government.

(b) The number of individuals that each agency determines are eligible for access to national security information will be kept to the absolute minimum required for the conduct of agency functions.

(1) Such eligibility will be granted only to those individuals who require access to national security information in order to perform official duties. This "need for access" shall be specifically justified by supervisory personnel in writing for approval by security officials and shall be recertified at least annually. However, the head of any agency may satisfy this requirement by personally certifying in writing that the functions of the organization, or any component thereof, require every individual within the organization or component to have access to national security information. Such certification shall be renewed at least biennially and filed with the Director of the Information Security Oversight Office.

(2) Annual performance ratings of supervisory personnel who certify an individual's "need for access" shall include an element concerning their performance of this function.

(3) Eligibility for access to national security information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the individual involved has no need for access to national security information and such access may reasonably be prevented. Instead, where circumstances indicate individuals may be inadvertently exposed to national security information in the course of their duties or where there is a potential risk to the national security that is independent of access to specific classified information, agencies are authorized to grant or deny, in their discretion, facility access approvals to such individuals based upon an appropriate level of investigation as determined by each agency.

(4) Eligibility for access to national security information shall not be requested or granted based upon a merely speculative need for access. Acquiring eligibility approvals for contingency purposes in excess of actual requirements is prohibited.

(5) Eligibility for access to national security information may be granted where there is a temporary need for access, such as one-time participation in a classified project, and the investigative standards prescribed by this Order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to national security information shall be limited to information related to the particular project or assignment. The access eligibility approval shall be annotated with these conditions.

Section 1.2 Level of Access Approval

(a) Approvals of eligibility for access to national security information may be granted at three levels: Confidential, Secret, or Top Secret. Access to Secret or Top Secret information shall authorize access to any lesser level of national security information.

(b) The level at which an access approval is granted shall be limited, and relate directly, to the level of national security information to which access is sufficiently justified as clearly necessary for the performance of official functions.

(c) Access to national security information relating to a special access program established under Executive Order 12356 of April 2, 1982, entitled "National Security Information", and its predecessors and successors may be granted in accordance with procedures established by the agency heads who created the program. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards established by this Order.

Section 1.3 Limited Access to Higher Levels

(a) An individual who has been deemed to be eligible for access to national security information based on adjudication of a completed investigation may be granted access to a higher level where such access

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 60 days;

(3) is limited to specific, identifiable information that is made the subject of a written access record; and

(4) is approved in writing by the agency head or senior officials designated in writing by the agency head to approve such access.

(b) Where the access granted under this section involves another agency's national security information, that agency shall be notified in advance of such access.

Section 1.4 Observance of Access Determinations By Other Agencies

(a) Except in cases where an agency has substantial information indicating that the individual may not satisfy the standards in Section 6.1 of this Order, an individual who has been deemed eligible for access to national security information in accordance with the procedural and investigative standards established by this Order should not be denied access to information classified at that level by another agency so long as such access is required in the performance of the official functions of the organization that granted the access.

(b) This Section shall not be applicable in situations where eligibility for access has previously been denied or revoked by another agency nor shall it preclude agencies from establishing additional investigative or adjudicative standards for candidates for detail or assignment to, employment at, or contractual work for such agencies.

Section 1.5 Specific Access Requirement

Except as provided in Section 4.3 of Executive Order 12356, or its successors, individuals who have been determined to be eligible for access to national security information shall only be given access to specific information that is necessary for the performance of official duties. It is the responsibility of persons who are in control of such information to determine that eligibility for access and this "need to know" exist prior to allowing such access and to challenge requests for access that do not appear to be well-founded.

(FORMERLY § 3.3)

Section 1.6 Access by Aliens

(a) Immigrant aliens and foreign nationals who contract with or are employed by the United States Government are not eligible for the same type of access eligibility approval that is granted to United States citizens but may only be provided with Limited Access Authorizations which shall authorize access only for specific programs, projects or contracts for which access to national security information is needed. Such authorizations may not make such individuals eligible for access to any greater level of national security information than the United States Government has determined may be released to the country of which the subject is currently a citizen and may be approved only where at least the prior ten years of the subject's life are amenable to investigation. Furthermore, if access above the Confidential level is involved, or there are any doubts concerning granting access, additional lawful investigative procedures should be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior official designated under Section 8.3 of this Order for compelling national security reasons that outweigh any risk of unauthorized disclosure.

Part 2

Determination of Eligibility for Access

Section 2.1 Standards

(a) No individual shall be deemed to be eligible for access to national security information merely by reason of federal service or contracting, licensee, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position or affiliation.

(b) Except as provided in Sections 3.2(a) and 3.3(a), eligibility for access to national security information shall be granted only to United States citizens as to whom a background investigation has been completed and whose personal and professional history affirmatively

indicates loyalty to the United States, strength of character, trustworthiness, reliability, discretion, and sound judgment, as well as demonstrated freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use and handling of national security information. A determination of eligibility for access to such information is a wholly discretionary security determination and may be granted based on judgments by appropriately trained security personnel only where the facts and circumstances indicate such access is clearly consistent with the national security interests of the United States.

Section 2.2 Basis for Eligibility Approval

Access eligibility determinations shall be based upon information concerning the subject that is acquired through the investigative procedures described in this Order or otherwise available to security officials. To the fullest extent possible, candidates for access will be responsible for providing affirmative evidence of their background, qualifications and character for use in investigating and adjudicating requests for access.

Part 3

Minimum Investigative Standards

Section 3.1 Initial Investigations

(a) All individuals who are to be considered for eligibility for access to national security information shall complete and submit to the relevant security officials a personal history statement and consent forms necessary to form the basis for an investigation into the background and character of the subject. This statement shall be designed to elicit the types of information concerning the history, character, and background of the individual upon which to base an investigation that will be necessary to determine whether the subject meets the standards established by this Order for access to national security information.

(b) Information concerning individuals who have been determined to have a justifiable need for access to Confidential or Secret information in the performance of official functions will be acquired through the conduct of an investigation consisting, at a minimum, of a review of records in the possession of the appropriate departments and agencies of the United States Government including the Security Investigations Index and FBI fingerprint and investigative files, and written inquiries of or personal contacts with financial and credit sources, state and local agencies, and present and former employers of the subject. Degrees awarded and diplomas received shall be verified. Where deemed productive and advisable in the interests of greater security, agencies should conduct other lawful investigative procedures, such as a subject interview and inquiries of neighbors, coworkers, or other persons who are familiar with the subject.

(c) Additional information will be acquired concerning individuals who have been determined to have a justifiable need for access to Top Secret information in the performance of official functions through the conduct of an expanded investigation that includes all the investigative procedures described in subsection (b) above, but involves personal contacts with, rather than written inquiries of, relevant sources of information concerning the subject's background, character and activities, as well as a personal interview of the subject by appropriately trained investigative or security personnel. Agencies are encouraged to conduct any other lawful investigative procedure.

(d) The time period covered by these investigations shall be at least the prior seven years of the individual's life or the time since the individual's sixteenth birthday, whichever is shorter. Agencies may, in their discretion, cover a lengthier time period in these investigations.

(e) Any credible information indicating the individual may not satisfy the standards established by this Order for access to national security information shall be fully pursued through additional lawful investigative procedures.

(f) To the fullest extent possible, information to be verified through an investigation will be acquired directly from the subject, either by means of the personal history statement or through oral or written contacts.

Section 3.2 Special Circumstances

(a) In emergency situations where official functions must must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to national security information may be granted to an individual for up to 120 days while the initial investigation is under way, if the agency head or a senior official designated in writing by the agency head finds in writing that such action is essential in the national interest. This finding shall be made a part of the agency records.

(1) A request for such a waiver must contain a detailed justification. The subject must be notified in writing that further access is expressly conditioned upon issuance of an access eligibility approval and will be immediately terminated, along with any assignment requiring an access eligibility approval, if such eligibility is not granted.

(2) Temporary eligibility for access may be granted only in consultation with the appropriate security officer based, at a minimum, on a personal interview of the subject, a review of FBI fingerprint and investigative files and the subject's personal history statement, and contact with the subject's last employer or other persons who are sufficiently familiar with the subject to vouch for the individual's integrity.

(3) Temporary eligibility for access may only be granted to particular, identified categories of national security information necessary to perform the official functions that are the bases for the action and not to all such information.

(4) If the investigation cannot be completed within the first 120-day period, temporary access eligibility may be extended for a limited period of time not to exceed 60 days.

(b) When one of the minimum investigative requirements prescribed in this Order cannot be satisfied in an individual case for reasons, other than lack of resources, beyond the control of the investigative agency (e.g., inability to investigate a period of foreign residency or citizenship, potential disclosure of national security information by fulfilling the investigative procedure, etc.), the particular investigative procedure may be waived by the senior official in each agency designated under Section 8.3(a) of this Order or a senior designee. Prior to considering such a waiver, however, every effort must be made to secure the information in question by other lawful investigative procedures. No such waiver shall be granted in the absence of a personal interview of the individual by security personnel. All waivers shall be made a part of the department or agency records.

(c) Access eligibility at the same level may be reapproved without further investigation as to individuals who were deemed to be eligible within the prior five years, provided they have remained employed by the same employer during the period in question, and that employer is aware of no information that would tend to indicate the subject may no longer satisfy the standards established by this Order for access to national security information. Access eligibility may be reapproved for individuals who have been retired or otherwise separated from United States Government employment for one year or less so long as there is no indication the subject may no longer satisfy the standards of this Order. A reinvestigation of the subject is necessary in any case if access to Top Secret information is required and over five years have passed since the last investigation of the subject.

Part 4

Reinvestigations

Section 4.1 Reinvestigative Requirements

(a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of individuals for access to national security information, reinvestigations shall be conducted with the same high priority and care as initial investigations.

(b) Individuals who are eligible for access to national security information may be the subject of reinvestigation any time there is reason to believe that they may no longer meet the standards for access that are established in this Order.

(c) All individuals who have been determined to be eligible for access to national security information shall submit updated personal history statements and consent forms to the appropriate security office as required by that Office but no less than every five years and shall also notify the security office in a timely manner any time there is a change or addition to the information provided in the subject's previous statement.

(d) Whenever any agency, contractor, licensee, or grantee becomes aware of information that raises doubts as to whether an individual's continued eligibility for access to national security information is clearly consistent with the interests of national security, such information shall be forwarded to the head of the agency that granted such access.

Section 4.2 Techniques for Reinvestigations

(a) Individuals who are eligible for access to Top Secret information will be the subject of a reinvestigation at least every five years based upon a current personal history statement and consent forms necessary to support such a reinvestigation. Such reinvestigations shall, at a minimum, include a personal interview by an appropriately trained security officer or investigator, a review of records in the possession of the appropriate departments and agencies of the United States Government, including the Security Investigations Index and FBI fingerprint and investigative files, and written inquiries or personal contacts with state and local agencies, financial and credit sources, and neighbors, coworkers, or other persons who are familiar with the subject. Where deemed to be productive and advisable in the interests of greater security, agencies should include any other lawful investigative procedures in the reinvestigation.

(b) Individuals who are eligible for access to Secret information will, to the extent permitted by resources, be reinvestigated every five years but, in any event, not less than once every ten years. Such reinvestigations shall include all the investigative procedures described in subsection (a) above, not including, however, the personal interview unless information developed by other means is deemed to warrant such an interview. Where deemed to be productive and advisable in the interests of greater security, agencies should include any other lawful investigative procedures in the reinvestigation.

Part 5

Investigations for Foreign Governments

Section 5.1 Authority

In order to facilitate investigations on behalf of the United States concerning periods of foreign residency or employment by friendly foreign governments and in the interest of foreign relations, agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the subject.

Part 6

Adjudication

Section 6.1 General Adjudication Criteria

(a) Among the factors to be considered in determining whether access to national security information should be granted or continued are whether the individual (1) has exploitable vulnerabilities or has engaged in any exploitable conduct or indiscreet behavior; (2) has demonstrated trustworthiness, reliability, excellent character and judgment; (3) has engaged in criminal or dishonest activity, alcohol or substance abuse, or exploitable sexual conduct; (4) has a history of mental, emotional, and financial stability; (5) is of unquestioned loyalty to the United States and not susceptible to undue influence, coercion, or duress.

(b) Executive Branch security officials should also consider the activities of any persons or groups with with the individual is bound by ties of affection, or with whom the individual is in close and continuing contact, and the activities of any persons in the individual's immediate family to determine the individual's susceptibility to influence, coercion or duress. Also to be considered is whether or not any such persons are foreign nationals, maintain dual citizenship, or reside in a foreign country.

(c) DELETED

Section 6.2 Adjudication of Initial Investigations

(a) All pertinent information including that obtained from the personal history statement supplied by the individual applying for access to national security information and the investigative procedures under this Order shall be made available to appropriately trained security personnel at the department or agency that is responsible for granting or denying the desired eligibility for access. These personnel must review the material for completeness and adherence to the requirements of this Order.

(b) Any information tending to indicate that the subject may not meet the standards for access eligibility that are established under this Order must be pursued and clarified until such point as the matter is resolved or security personnel are satisfied that further inquiries would be fruitless. A personal interview, written exchange of information with the subject, or other lawful investigative procedures should be used to resolve questionable areas.

(c) At such time as the investigation is deemed to be complete, security personnel will review and consider the available information in its entirety in order to determine whether, in their judgment, the subject possesses the qualities that are described in this Order and that merit the high trust and confidence that is vested in those individuals who are granted eligibility for access to national security information. Where there is reasonable doubt concerning these matters or sufficient information cannot be developed to evaluate an individual under these standards, such access eligibility will be denied.

Section 6.3 Periodic Review of Personal History Information

Appropriately trained security personnel will review personal history information provided under section 4.1(c) of this Order by individuals who have been granted eligibility for access to national security information. Any areas that are deemed to warrant clarification shall be pursued with the subject personally and, if necessary, through lawful investigative procedures.

Section 6.4 Adjudication of Reinvestigations

(a) When reinvestigation is required under section 4.2 of this Order, all pertinent information shall be reviewed to determine whether there has been any change in the facts and circumstances that originally served as the basis for the approval, or for the most recent reapproval, of the subject's eligibility for access to national security information.

(b) Any information tending to indicate the subject may no longer meet the standards for access eligibility established under this Order shall be pursued either with the subject directly or through lawful investigative procedures. If deemed advisable by security personnel, the subject's access eligibility may be suspended pending the outcome of these inquiries.

(c) At such time as the reinvestigation is considered to be complete, security personnel shall review it in its entirety to determine whether, in their judgment, the subject continues to meet the standards established under this Order and whether continued eligibility for access to national security information is warranted. Where there is reasonable doubt concerning these matters, access eligibility will be denied.

Section 6.5 Effect of Adjudication

The security official's determinations will be explained in agency records as fully as is consistent with the national security interests of the United States and appropriately filed. A determination that the subject is not eligible for access to national security information does not by itself disqualify the subject for federal employment or contracting opportunities that do not require such access.

Part 7

Appeals

Section 7.1 Determinations of Need for Access

A determination that an individual does not have or no longer has a need for eligibility for access to national security information in order to perform official functions is entirely within the discretion of the sponsoring agency and shall be conclusive.

Section 7.2 Determinations of Eligibility for Access

Individuals except candidates for initial access or for access at a higher level who are determined not to meet the standards established in this Order for access to national security information, shall be provided:

(a) as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States permit;

(b) reasonable opportunity to reply in writing under oath or affirmation and request a review of the determination;

(c) written notice of the results of the review and the identity of the deciding authority; and

(d) an opportunity to appeal in writing to a higher authority, appointed by the agency head, whose decision shall be final.

Section 7.3 Discretionary Authority, Exceptions

(a) Agency heads may, at their sole discretion and as resources and national security considerations permit, provide for additional review proceedings such as hearings, opportunities to confront persons making statements adverse to the subject and appearance by legal counsel. These additional procedures are not required, however, and this section is intended to create no procedural or substantive rights.

(b) The procedures set forth in Section 7.2 shall not be made available where the head of an agency or the senior official under Section 8.3(a) certifies that to do so would damage the national security interests of the United States.

(c) Consistent with the National Security Act of 1947, the procedures set forth in Section 7.2 of this Order shall not be made available to any individual whose eligibility for access is adjudicated by the Central Intelligence Agency where the Director of Central Intelligence determines that to do so would not be necessary or advisable in the interests of the United States.

(d) Consistent with section 303 of the Internal Security Act of 1950, as amended, the procedures set forth in Section 7.2 of this Order shall not be made available to any individual whose eligibility for access is adjudicated by the National Security Agency where the Director of the National Security Agency determines that to do so would not be consistent with the national security.

Part 8

Implementation and Review

Section 8.1 National Security Council

(a) The National Security Council shall review and provide overall policy direction for the federal personnel security program established under this Order.

(b) The Administrator of the General Services Administration shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate these functions to the Director of the Information Security Oversight Office established by Executive Order 12356.

Section 8.2 Information Security Oversight Office

In addition to the duties set forth in Executive Order 12356, the Director of the Information Security Oversight Office shall:

(a) develop, in consultation with the agencies, and promulgate, subject to the approval of the

National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(b) oversee agency actions to ensure compliance with this Order and implementing directives;

(c) review all agency implementing regulations. The Director shall require any regulation to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation shall remain in effect pending a prompt decision on the appeal;

(d) have the authority to conduct on-site reviews of the personnel security program of each agency and to require of each agency under appropriate security safeguards such reports, information, and other cooperation as may be necessary to fulfill the Director's responsibilities. If it is determined that a report, inspection, or access to specific information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 8.3(a) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(e) monitor the number and level of access eligibility approvals granted by each agency of the Government and bring to the attention of the agency head any significant, unexplained increase in the number of such approvals granted;

(f) oversee and monitor the adjudication policies of the various agencies to ensure, to the extent practicable, uniformity of policy;

(g) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the personnel security program, but not including action on specific agency determinations concerning the eligibility of individuals for access to national security information.

(h) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of an effective federal personnel security program;

(i) report at least annually to the President through the National Security Council concerning implementation of this Order;

(j) have the authority to convene and chair inter-agency meetings to discuss matters pertaining to the federal personnel security program created under this Order; and

(k) review and make recommendations to the National Security Council and the President concerning any request or effort by an organization, other than those properly authorized to perform such functions at the date of this Order, to perform or contract for personnel security investigations required under this Order.

Section 8.3 Agency Implementing Responsibilities

Heads of agencies that grant individuals eligibility for access to national security information shall:

(a) designate a senior agency official to direct and administer the personnel security program established by this Order. All such programs shall include an active oversight and continuing security education and awareness program to ensure effective implementation of this Order;

(b) promulgate implementing regulations no later than 120 days from the effective date of this Order that provide for the heightened personnel security program that is the goal of this Order.

(c) ensure that any regulations authorizing use of the polygraph under this Order include procedures to control the circumstances under which polygraph examinations may be administered for purposes of this Order, ensure that results of such examinations are disseminated only to those persons necessary to achieve the purposes

of this Order or fulfill obligations to report possible violations of criminal laws, enhance the accuracy of examination results, provide safeguards to ensure reliable polygraph results, limit the scope of the examination to counterintelligence questions, and to require, as appropriate, that persons be informed prior to the examination that they are entitled to invoke their Fifth Amendment right not to answer a particular question and to ask that a particular question be rephrased.

(d) establish procedures to require that a demonstrable need for access to national security information is clearly established before granting eligibility for access, ensure that persons who review requests for access eligibility carefully evaluate the justification presented and challenge inadequate requests, and to limit the number of individuals granted access to such information to the absolute minimum consistent with operational requirements.

(e) establish and maintain continuing training programs for employees who conduct investigations, request access approvals, or review investigative files to determine whether eligibility for access to national security information should be granted;

(f) cooperate, under the guidance of the Director of the Information Security Oversight Office, with other agencies to achieve practical, consistent and effective adjudicative training and standards; and

(g) institute procedures to ensure that credible indications of potential espionage or terrorist activities or similar threats to the national security are referred to or coordinated with the Federal Bureau of Investigation.

(h) DELETED

Section 8.4 Individual Responsibilities

(a) Individuals who are granted eligibility for access to national security information occupy positions of high trust and confidence and shall:

(1) report all contacts with persons, including foreign nationals, who are interested in obtaining unauthorized access to classified information;

(2) report all foreign travel prior to departure to the appropriate security official;

(3) report all violations of security regulations to the appropriate security official;

(4) challenge in writing to the appropriate approval authority questionable requests for access eligibility or need to know determinations;

(5) assist in limiting the number of access eligibility requests and approvals to the absolute minimum necessary to meet operational requirements; and

(6) fulfill the requirements of section 4.1(c) in a timely manner.

(b) Supervisors of employees who have been granted eligibility for access to national security information shall continually assess the status of those employees and report any circumstances that might indicate the development of a personnel security concern, to include violations of security regulations, sudden and unexplained affluence, recurrent and unexplained foreign travel, excessive indebtedness, sustained mental or emotional problems, drug use, or excessive use of alcoholic beverages, to the appropriate security officer.

Section 8.5 Sanctions

(a) Whenever the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, a report shall be made to the head of the agency or to the senior official designated under Section 8.3(a). These officials will ensure that appropriate corrective steps are taken.

(b) Officers and employees of the United States Government and its contractors, licensees, and grantees, and military personnel shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for or allow access to national security information in violation of this Order. Sanctions shall be imposed promptly and may include reprimand, suspension without pay, removal, and other sanctions in accordance with applicable law and agency regulation. The Director of the Information Security Oversight Office shall be notified in a timely manner of such violations, remedial actions and sanctions imposed.

Part 9

General

Section 9.1 Provisos

(a) Nothing in this Order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the minimum investigative requirements set forth in this Order. Furthermore, agencies have an obligation to seek further information as necessary to resolve issues that may arise during the course of an investigation or reinvestigation.

(b) Nothing in this Order shall limit the authority of the Central Intelligence Agency, the National Security Agency, or the Federal Bureau of Investigation to continue to use polygraph interviews of a scope those agencies deem appropriate to their personnel security programs.

(c) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. Access to "Restricted Data" and "Formerly Restricted Data" shall be granted in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(d) Nothing in this Order shall prohibit the granting of temporary, limited access to national security information if such access is necessary to carry out or protect specific intelligence or counterintelligence operations. Such access shall be granted under procedures approved by the head of an agency engaged in such activities.

(e) Nothing in this Order shall apply to members of Congress or Federal judges appointed by the President and confirmed by the Senate, or to the processes established under the Classified Information Procedures Act.

Section 9.2 Interpretation

(a) The Attorney General, upon request of the National Security Council, the head of an agency, or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

Section 9.3 Purpose and Effect

(a) This Order is intended to provide uniform standards to govern access to national security information and does not affect any employment suitability or other security program.

(b) The authority to grant eligibility for access to national security information is wholly discretionary and, except as explicitly and specifically provided, nothing contained in this Order or in procedures implementing the provisions of this Order is intended to confer any substantive or procedural rights or privileges on any person or organization.

(c) This Order shall become effective on (120 after signing).

Section 9.4 Revocation

Sections 2 through 9 of Executive Order 10865, entitled "Safeguarding Classified Information in Industry," are hereby revoked.